Confidential

Subject: ISOC Blue Advisory – November 28, 2006 Excerpted from SANS Critical Vulnerabilities

Severity: Low

What: November 28, 2006 Excerpted from SANS Critical Vulnerabilities

Action: This is a notification from the ISOC for your information

Current Status: These are current as of 11/28/2006

ISOC Next Steps: If you have any questions please contact the ISOC.

Additional Information: November 28, 2006 Excerpted from SANS Critical Vulnerabilities

(1) HIGH: Mac OS X Disk Image Kernel Memory Corruption
Affected:
Mac OS X current version and possibly all prior versions

Description: The "Month of Kernel Bugs (MoKB)" project has discovered a memory corruption flaw in the Mac OS X that can be triggered when the OS X loads a specially crafted "disk image (DMG)" file. The vulnerability can be exploited to execute arbitrary code with kernel privileges. Note that the flaw can be exploited remotely via Safari browser. Safari, in its default configuration, treats disk image files as safe and opens them automatically. Hence, a website containing a malicious disk image file can compromise a Mac OS X client. A proof-of-concept exploit has been publicly posted.

Status: Apple has not confirmed, no updates available. The remote attack vector via Safari can be mitigated by turning off the "Open Safe Files" feature in Safari. However, by turning this feature off, the user would be prompted every time before opening files such as movies and PDFs.

Council Site actions: Only one of the responding council sites is using the affected software. They have Safari configured with "Open safe files" turned off. They will deploy they patches when they become available

References:
Month of Kernel Bugs (Discovered by "File Format Fuzzing") http://projects.info-pull.com/mokb/MOKB-20-11-2006.html
Proof of Concept Disk Image
http://www.securityfocus.com/data/vulnerabilities/exploits/MOKB-20-11-2006.dmg.bz2
SecurityFocus BID
http://www.securityfocus.com/bid/21201

(2) HIGH: Acer Notebooks ActiveX Control Arbitrary Command Execution
Affected:
All Acer Notebooks running Windows

Description: Acer, a Taiwan based company, is a leading Notebook producer with a dominant presence in the Europe, Asia and Africa (EMEA) market. Acer Notebooks ship with "LunchApp.APlunch" ActiveX control that is marked as safe for scripting. This ActiveX control supports "Run"
method that can be used to run any command (with arbitrary parameters) on an Acer notebook remotely. A specially crafted webpage or an HTML email can exploited this flaw to compromise Acer Notebooks. The discoverer has posted a proof-of-concept exploit, and tested the presence of this ActiveX control on an older as well as a more recent Acer model.

Status: Acer has not confirmed. A workaround is to set the kill bit for the LunchApp.APlunch ActiveX control's UUID:
D9998BD0-7957-11D2-8FED-00606730D3AA.

Council Site Actions: The affected software and/or configuration are not in production or widespread use, or are not officially supported at any of the council sites. They reported that no action was necessary.

References:
Advisory by Tan Chew Keong (includes PoC exploit) http://vuln.sg/acerlunchapp-en.html
Setting Killbit for an ActiveX Control
http://support.microsoft.com/kb/240797
Acer Home Page
http://global.acer.com/
SecurityFocus BID
http://www.securityfocus.com/bid/21207

(3) MODERATE: Computer Associates BrightStor ARCserve Backup Buffer Overflow
Affected:
BrightStor ARCserver Backup version 11.5 and possibly prior

Description: Computer Associates BrightStor ARCserve Backup products provide backup services for Windows, NetWare, Linux and UNIX. The products contains a buffer overflow that can be triggered by a specially crafted RPC request to the port 6502/tcp. The flaw can be exploited to execute arbitrary code with SYSTEM privileges. The technical details have not been publicly posted yet.

Status: CA is aware of this issue and is working on a fix. A workaround, in the meanwhile, is to block the requests to port 6502/tcp at the network perimeter.

Special Note: CA backup products have been reported to contain multiple vulnerabilities for the past few years. SANS recommends you to block all the ports that are opened by the software at the network perimeter. A list of the ports to block may be found at:
http://www.ca.com/at/local/partner/techtalk_mar05_faq.pdf
http://supportconnectw.ca.com/public/ca_common_docs/brightstorwinxpsp2matrix.asp

Council Site Actions: The affected software and/or configuration are not in production or widespread use, or are not officially supported at any of the council sites. They reported that no action was necessary.

References:
Posting by LSsec Security
http://archives.neohapsis.com/archives/bugtraq/2006-11/0418.html
Posting by James K Williams, CA

http://archives.neohapsis.com/archives/bugtraq/2006-11/0443.html
Product Page
http://www3.ca.com/Solutions/ProductList.asp?ID=4536&TYPE=P SecurityFocus BID
http://www.securityfocus.com/bid/21140

(4) MODERATE: RealNetworks Helix DNA Server Unspecified Buffer Overflow
Affected:
Helix DNA Server versions 11.0 and 11.1

Description: Real Network Helix DNA Server, a popular media streaming server, contains a heap-based buffer overflow. According to the discoverer, the flaw can be exploited to execute arbitrary code with the privileges of the server process, often root. No technical details about the vulnerability have been publicly released yet. The exploit details are reportedly available to the users of the "vulndisco" pack.

Status: Vendor not confirmed.

Council Site Actions: The affected software and/or configuration are not in production or widespread use, or are not officially supported at any of the council sites. They reported that no action was necessary.

References:
Helix Community Home Page
http://helixcommunity.org/
Vulndisco Pack
http://www.gleg.net
SecurityFocus BID
http://www.securityfocus.com/bid/21141

****
Other Software
****

(5) HIGH: GNU Radius Format String Vulnerability
Affected:
GNU Radius versions prior to 1.4

Description: GNU Radius is a server for user authentication and accounting. The server supports SQL databases for authentication and accounting. The Radius server contains a format string vulnerability when it is compiled with a SQL back-end, and the SQL accounting is turned on. The flaw can be exploited by unauthenticated attackers to execute arbitrary code on the server with typically root privileges. The technical details can be extracted by examining the fixed and the vulnerable versions of the server code.

Status: GNU has released version 1.4 to fix this flaw. Note that the FreeBSD and Gentoo Linux versions are vulnerable in their default configuration.

References:
iDefense Advisory
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=443
GNU Radius Homepage
http://www.gnu.org/software/radius/
SecurityFocus BID

Not yet available.

(6) HIGH: Un4Seen XMPlay M3U Buffer Overflow
Affected:
XMPlay version 3.3.0.4

Description: XMPlay, an audio player for Windows systems, contains a stack-based buffer overflow. The overflow can be triggered by a media file (".m3u", ".pls" or ".asx" file extensions) containing an overlong media filename, and exploited to execute arbitrary code with the privileges of the logged-on user. Multiple exploits have been publicly posted.

Status: Vendor has not confirmed, no updates available. The current version on the vendor's site is 3.3.0.5, and the discoverer(s) of this 0-day flaw have reported version 3.3.0.4 to be vulnerable. Hence, it is likely that the current version is not affected.

Council Site Actions: The affected software and/or configuration are not in production or widespread use, or are not officially supported at any of the council sites. They reported that no action was necessary.

References:
Exploit Code
http://downloads.securityfocus.com/vulnerabilities/exploits/xmplay_exploit.c
http://downloads.securityfocus.com/vulnerabilities/exploits/XMPlay_ASX_Exploit.c
Un4Seen Home Page
http://www.un4seen.com/
M3U and ASX File Format
http://www.mediacollege.com/video/format/windows-media/files/asx.html
http://forums.winamp.com/showthread.php?threadid=65772
SecurityFocus BID
http://www.securityfocus.com/bid/21206

(7) HIGH: NetGear WG311v1 Wireless Driver SSID Buffer Overflow
Affected:
NetGear WG311v1 wireless driver version 2.3.1 10 and possibly prior

Description: The NetGear WG311v1 device driver, used to control NetGear wireless cards, contains a buffer overflow vulnerability. By sending a specially-crafted 802.11 (WiFi) frame containing an overly long SSID, an attacker could exploit this buffer overflow and take complete control of the vulnerable system. No authentication is required, and attackers need only be within wireless range of the vulnerable system. Because this vulnerability lies within the processing of probe response packets, the victim does not need to explicitly connect to a malicious wireless network to be exploited. This driver is primarily designed for Microsoft Windows systems, but it is believed to be compatible with the "NdisWrapper" cross-platform driver framework, making it possible to run this driver under Linux (and possibly other operating systems) on the Intel platform. This vulnerability was discovered as part of a project to discover bugs in various operating systems' kernels. A working exploit is available for this vulnerability. This vulnerability is similar to several discovered for other NetGear wireless device drivers that were documented in a previous issue of @RISK.

Status: NetGear has not confirmed, no updates available.

References:
Month of Kernel Bugs Advisory
http://projects.info-pull.com/mokb/MOKB-22-11-2006.html
Metasploit Module
http://metasploit.com/svn/framework3/trunk/modules/auxiliary/dos/wireless/netgear_wg311pci.rb
NetGear Home Page
http://www.netgear.com
Wikipedia Entry on Device Drivers
http://en.wikipedia.org/wiki/Device_driver
Ndis Home Page
http://ndiswrapper.sourceforge.net
Previous @RISK Entry
http://www.sans.org/newsletters/risk/display.php?v=5&i=46#other1
SecurityFocus BID
http://www.securityfocus.com/bid/21251

Weekly Comprehensive List of Newly Discovered Vulnerabilities

Windows
06.47.1 CVE: Not Available
Platform: Windows
Title: XMPlay Playlist Files Remote Buffer Overflow
Ref: http://www.securityfocus.com/bid/21206/info

06.47.2 CVE: Not Available
Platform: Windows
Title: Novell Client Unspecified NWSPOOL.DLL Buffer Overflow
Ref: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2974765.htm

Third Party Windows Apps
06.47.3 CVE: Not Available
Platform: Third Party Windows Apps
Title: Conti FTP Insecure Default Accounts and Directory Traversal Vulnerabilities
Ref: http://www.securityfocus.com/bid/21174

06.47.4 CVE: Not Available
Platform: Third Party Windows Apps
Title: Tftpd32 Filename Remote Buffer Overflow
Ref: http://www.securityfocus.com/bid/21148

06.47.5 CVE: Not Available
Platform: Third Party Windows Apps
Title: Knownsoft Turbo Searcher ARJ File Handling Buffer Overflow
Ref: http://www.securityfocus.com/bid/21208

Mac OS
06.47.6 CVE: CVE-2006-4413
Platform: Mac Os
Title: Apple Remote Desktop Insecure Default Package Permission
Ref: http://www.securityfocus.com/bid/21139

06.47.7 CVE: Not Available

Platform: Mac Os
Title: Mac OS X UDIF Disk Image Remote Code Execution
Ref: http://kernelfun.blogspot.com/2006/11/mokb-20-11-2006-mac-os-x-apple-udif.html

Linux
06.47.8 CVE: Not Available
Platform: Linux
Title: Dovecot IMAP Server Mapped Pages Off-By-One Buffer Overflow
Ref: http://www.securityfocus.com/archive/1/452081

06.47.9 CVE: Not Available
Platform: Linux
Title: Kile Backup File Insecure File Permissions
Ref: http://www.securityfocus.com/bid/21200

06.47.10 CVE: Not Available
Platform: Linux
Ref: https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=206736

BSD
06.47.11 CVE: Not Available
Platform: BSD
Title: OpenBSD LD.SO Local Environment Variable Clearing
Ref: http://www.securityfocus.com/bid/21188

UNIX
06.47.12 CVE: Not Available
Platform: Unix
Title: IBM OS/400 ASN.1 Parser Multiple Unspecified Vulnerabilities
Ref: http://www.securityfocus.com/bid/21189

Cross Platform
06.47.13 CVE: CVE-2006-5868
Platform: Cross Platform
Title: ImageMagick SGI Image File Unspecified Remote Heap Buffer Overflow
Ref: http://www.securityfocus.com/bid/21185

06.47.14 CVE: CVE-2006-3093
Platform: Cross Platform
Title: Acrobat Reader DLL Multiple Denial Of Service Vulnerabilities
Ref: http://www.securityfocus.com/bid/21155/info

06.47.15 CVE: Not Available
Platform: Cross Platform
Title: IBM WebSphere Application Server Multiple Vulnerabilities
Ref: http://www.securityfocus.com/bid/21204

06.47.16 CVE: Not Available
Platform: Cross Platform
Title: Fuzzball MUCK Message Parsing Interpreter Buffer Overflow
Ref: http://www.securityfocus.com/bid/21217

06.47.17 CVE: Not Available
Platform: Cross Platform
Title: GNU Tar GNUTYPE_NAMES Remote Directory Traversal
Ref: http://www.securityfocus.com/bid/21235

Web Application

06.47.18 CVE: CVE-2006-2311
Platform: Web Application - Cross Site Scripting
Title: CPanel DNSlook.HTML Cross-Site Scripting
Ref: http://www.securityfocus.com/archive/1/451931

06.47.19 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: Travelsized CMS Index.PHP Multiple Cross-Site Scripting Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/452007

06.47.20 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: vBulletin Admin Control Panel Index.PHP Multiple Cross-Site Scripting Vulnerabilities
Ref: http://www.securityfocus.com/bid/21157

06.47.21 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: Bloo Googlespell_Proxy.PHP Cross-Site Scripting
Ref: http://www.securityfocus.com/archive/1/451777

06.47.22 CVE: Not Available
Platform: Web Application - Cross Site Scripting
Title: Eggblog Multiple Cross-Site Scripting Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/451863

06.47.23 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Powie's PHP Forum EditPoll.PHP SQL Injection
Ref: http://www.securityfocus.com/bid/21144

06.47.24 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Image Gallery with Access Database Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/bid/21131

06.47.25 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Oxygen O2PHP Bulletin Board ViewThread.PHP SQL Injection
Ref: http://www.securityfocus.com/bid/21172

06.47.26 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Enthrallweb EClassifieds Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/452102

06.47.27 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Gnews Publisher Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/452116

06.47.28 CVE: Not Available
Platform: Web Application - SQL Injection
Title: Klf-Realty Multiple SQL Injection Vulnerabilities
Ref: http://klf-design.com/

06.47.29 CVE: Not Available
Platform: Web Application
Title: PHPMyAdmin Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/bid/21137

06.47.30 CVE: Not Available
Platform: Web Application
Title: BirdBlog Multiple Cross-Site Scripting Vulnerabilities
Ref: http://www.securityfocus.com/bid/21184

06.47.31 CVE: CVE-2006-5767
Platform: Web Application
Title: MyAlbum Language.Inc.PHP Remote File Include
Ref: http://www.securityfocus.com/archive/1/452140

06.47.32 CVE: Not Available
Platform: Web Application
Title: Boonex Dolphin Index.php Remote File Include
Ref: http://www.securityfocus.com/bid/21182/info

06.47.33 CVE: Not Available
Platform: Web Application
Title: dev4U CMS Index.PHP Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/bid/21170

06.47.34 CVE: Not Available
Platform: Web Application
Title: phpBB2 PlusXL Functions.PHP Remote File Include
Ref: http://www.securityfocus.com/archive/1/452012

06.47.35 CVE: Not Available
Platform: Web Application
Title: ActiveNews Manager Multiple Input Validation
Ref: http://www.securityfocus.com/bid/21167

06.47.36 CVE: Not Available
Platform: Web Application
Title: MosReporter Component Remote File Include
Ref: http://www.securityfocus.com/bid/21160

06.47.37 CVE: Not Available
Platform: Web Application
Title: Dicshunary Check_Status.PHP Remote File Include
Ref: http://www.securityfocus.com/bid/21162/info

06.47.38 CVE: Not Available
Platform: Web Application
Title: Sage IMG Element Input Validation
Ref: http://www.securityfocus.com/bid/21164

06.47.39 CVE: Not Available
Platform: Web Application
Title: DoSePa Information Disclosure
Ref: http://www.securityfocus.com/bid/21149

06.47.40 CVE: Not Available
Platform: Web Application

Title: PHP Upload Tool Arbitrary File Upload and Directory Traversal Vulnerabilities
Ref: http://www.securityfocus.com/bid/21150

06.47.41 CVE: Not Available
Platform: Web Application
Title: 20/20 Auto Gallery Multiple SQL Injection Vulnerabilities
Ref: http://www.securityfocus.com/bid/21154

06.47.42 CVE: Not Available
Platform: Web Application
Title: mxBB Calsnails Module MX_Common.PHP Remote File Include
Ref: http://www.securityfocus.com/bid/21143

06.47.43 CVE: Not Available
Platform: Web Application
Title: MG.Applanix APX_Root_Path Parameter Multiple Remote File Include Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/452138

06.47.44 CVE: Not Available
Platform: Web Application
Title: ASPNuke Register.ASP SQL Injection
Ref: http://www.securityfocus.com/bid/21195

06.47.45 CVE: Not Available
Platform: Web Application
Title: Alt-N MDaemon Local Insecure Default Directory Permissions
Ref: http://www.securityfocus.com/bid/21127

06.47.46 CVE: Not Available
Platform: Web Application
Title: Etomite CMS Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/451838

06.47.47 CVE: Not Available
Platform: Web Application
Title: Xtreme ASP Photo Gallery Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/451786

06.47.48 CVE: Not Available
Platform: Web Application
Title: Oliver LoginForm Inc.PHP Remote File Include
Ref: http://www.securityfocus.com/bid/21202

06.47.49 CVE: Not Available
Platform: Web Application
Title: Rapid Classified Multiple Input Validation Vulnerabilities
Ref: http://www.securityfocus.com/archive/1/452088

06.47.50 CVE: Not Available
Platform: Web Application
Title: phpQuickGallery Remote File Include
Ref: http://www.securityfocus.com/archive/1/452012

06.47.51 CVE: CVE-2006-5733
Platform: Web Application

Title: PostNuke Error.PHP Local File Include
Ref: http://community.postnuke.com/Article2787.htm

Network Device
06.47.52 CVE: Not Available
Platform: Network Device
Title: NetGear MA521 Wireless Driver Long Beacon Probe Buffer Overflow
Ref: http://www.kb.cert.org/vuls/id/395496

06.47.53 CVE: Not Available
Platform: Network Device
Title: NetGear WG111v2 Wireless Driver Long Beacon Buffer Overflow
Ref: http://www.kb.cert.org/vuls/id/445753

06.47.54 CVE: Not Available
Platform: Network Device
Title: RealNetworks Helix DNA Server Unspecified Buffer Overflow
Ref: http://www.securityfocus.com/bid/21141/info

Thank you,
Information Security Operations Center (ISOC)
isoc@state.co.us
(303) 866-3465

*"Information Security - Working Together to Make **IT** happen"*